					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P05					Titolo del documento: **Politica di gestione delle modifiche**							
Versione: 1.0		Data di entrata in vigore: 01.01.2025			Proprietario del documento:							
X	Politica		Standard		Procedura		Modulo		Registro		Altro	

Cronologia delle revisioni				
Numero di revisione	**Data di revisione**	**Modifiche**	**Riesaminato da**	**Proprietario del processo**

Approvazioni			
Nome	**Ruolo**	**Data**	**Firma**

Allineamento a standard e normative

Standard/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausole 6.1, 5.15	Riguarda le azioni sui rischi, il controllo degli accessi e la gestione delle modifiche
ISO/IEC 27002:2022	Controllo 8	Attua un processo strutturato di gestione delle modifiche
NIST SP 800-53 Rev.5	Da CM-2 a CM-14	Controlli di gestione della configurazione
GDPR UE	Articoli 32(1)(b–d), 25; Considerando 78	Misure tecniche e organizzative per la sicurezza di sistemi e dati durante le modifiche
NIS2 UE	Articolo 21(2)(a, b, d, e)	Impone la gestione del rischio delle modifiche ai sistemi ICT
DORA UE	Articoli 5, 8, 12	Disciplina il rischio operativo/ICT e la segnalazione degli incidenti
COBIT 2019	BAI06, BAI02, BAI03, DSS01, MEA01, MEA03	Gestione strutturata delle modifiche IT, prestazioni, conformità e requisiti

1. Finalità

1.1. La presente politica stabilisce un quadro formale per l'avvio, la valutazione, l'approvazione, l'attuazione e il riesame delle modifiche ai sistemi informativi, all'infrastruttura, alle applicazioni e ai processi correlati dell'organizzazione.

1.2. Essa garantisce che tutte le modifiche siano eseguite in modo controllato e verificabile ai fini di audit, minimizzando il rischio di interruzioni, compromissioni della sicurezza o non conformità normative.

1.3. Supporta il Controllo 8.32 dell'Appendice A della ISO/IEC 27001:2022 applicando pratiche di gestione delle modifiche sicure, documentate e allineate al rischio.

1.4. La politica garantisce inoltre la tracciabilità delle decisioni relative alle modifiche e promuove la resilienza operativa durante interventi pianificati o di emergenza.

2. Ambito di applicazione

2.1. La presente politica si applica a tutte le modifiche che interessano sistemi, dati e ambienti compresi nel campo di applicazione del SGSI, inclusi:

2.1.1. infrastruttura IT (on-premise, cloud, ibrida)

2.1.2. ambienti di produzione, pre-produzione e disaster recovery

2.1.3. applicazioni aziendali, servizi, API e integrazioni

2.1.4. impostazioni di configurazione, applicazione delle patch, rilasci software e migrazioni di sistema

2.1.5. correzioni di emergenza e modifiche pianificate o basate su progetto

2.2. Essa disciplina le modifiche avviate da:

2.2.1. personale interno (operazioni IT, sviluppatori, proprietari dei sistemi)

2.2.2. fornitori esterni, fornitori di servizi gestiti e collaboratori esterni

2.2.3. gruppi di progetto durante l’implementazione di sistemi, aggiornamenti o transizioni di servizio

2.3. La presente politica non si applica a:

2.3.1. ambienti temporanei di sviluppo e test senza accesso ai dati di produzione

2.3.2. configurazioni personali degli utenti (disciplinate dalla Politica sull’uso accettabile)

2.3.3. modifiche a sistemi esterni al perimetro di controllo dell’organizzazione, salvo che incidano su asset integrati o obblighi di conformità

3. Obiettivi

3.1. Garantire che tutte le modifiche siano riesaminate, approvate, testate e documentate prima dell’esecuzione.

3.2. Mantenere la disponibilità dei sistemi, l’integrità dei dati e la continuità dei servizi durante e dopo le attività di modifica.

3.3. Richiedere classificazioni delle modifiche definite, piani di rollback e valutazioni del rischio per tutte le tipologie di modifica.

3.4. Consentire processi decisionali trasparenti ed escalation mediante una governance strutturata.

3.5. Supportare la dimostrazione della conformità attraverso registrazioni delle modifiche tracciabili e riesami post-implementazione.

3.6. Applicare la segregazione dei compiti (SoD) e ridurre il rischio di modifiche non autorizzate o in conflitto nei sistemi critici.

4. Ruoli e responsabilità

4.1. Direzione esecutiva

4.1.1. Approva la Politica di gestione delle modifiche e ne assicura l’allineamento con gli obiettivi strategici e gli obblighi normativi.

4.1.2. Approva programmi di modifica ad alto impatto o trasversali nell’ambito della supervisione di governance.

4.1.3. Assegna le risorse e il budget necessari per gli strumenti di controllo delle modifiche e per la formazione del personale.

4.2. Comitato consultivo per le modifiche

4.2.1. Riesamina e autorizza le modifiche standard e le modifiche di maggiore rilievo, assicurando un’adeguata valutazione di rischi, impatti e dipendenze.

4.2.2. Convalida i piani di rollback, i risultati dei test, le comunicazioni alle parti interessate e la pianificazione.

4.2.3. È composto da proprietari dei sistemi, sicurezza delle informazioni, operazioni IT, referenti di business e rappresentanti della conformità.

4.2.4. Può delegare le decisioni per modifiche a basso rischio o di emergenza in condizioni documentate.

[... Le sezioni 4.3–8 non sono incluse in questa anteprima. Acquistare il documento completo per accedere all'intero contenuto. ...]

9. Requisiti di riesame e aggiornamento

9.1. Fattori scatenanti e frequenza del riesame

9.1.1. La presente politica deve essere riesaminata annualmente o in occasione di:

9.1.1.1. modifiche rilevanti dell’IT o dell’infrastruttura

9.1.1.2. incidenti significativi correlati a modifiche non riuscite o non autorizzate

9.1.1.3. aggiornamenti normativi o nuovi obblighi legali relativi alle modifiche

9.1.1.4. implementazione di nuovi strumenti o piattaforme del sistema di gestione delle modifiche

9.2. Processo di riesame della Politica di gestione delle modifiche

9.2.1. Il Responsabile delle modifiche guiderà il processo di riesame in collaborazione con:

9.2.1.1. IT, Sicurezza e Operazioni

9.2.1.2. audit interno e rischio

9.2.1.3. rappresentanti del Comitato consultivo per le modifiche

9.2.2. Gli aggiornamenti devono essere riesaminati e approvati dalla Direzione esecutiva e dal Comitato direttivo del SGSI.

9.2.3. Le versioni riemesse devono essere tracciate nel Registro dei documenti e comunicate alle parti interessate con nuova presa visione, ove necessario.

9.3. Controllo documentale e gestione delle versioni

9.3.1. Tutte le versioni devono includere:

9.3.1.1. ID della politica, titolo e livello di classificazione

9.3.1.2. proprietario e cronologia delle revisioni

9.3.1.3. registro delle modifiche e data di entrata in vigore

9.3.1.4. autorità di approvazione

9.3.2. Le versioni archiviate devono essere conservate in conformità alla Politica di conservazione dei documenti (minimo 3 anni).

10. Politiche correlate e collegamenti

10.1. La presente politica è direttamente collegata e supporta l'applicazione di:

10.1.1. P1 – Politica per la sicurezza delle informazioni: stabilisce il requisito di controlli formali di sicurezza e di responsabilità a livello di processo, inclusa la governance della gestione delle modifiche.

10.1.2. P2 – Politica su ruoli e responsabilità di governance: definisce le autorità di approvazione e la segregazione dei compiti rilevanti per l'autorizzazione e la supervisione delle modifiche.

10.1.3. P4 – Politica di controllo degli accessi: garantisce che le autorizzazioni di accesso per gli esecutori e i revisori delle modifiche seguano il principio del privilegio minimo.

10.1.4. P6 – Politica di gestione del rischio: garantisce che tutte le modifiche siano soggette a un'adeguata valutazione del rischio e a strategie di mitigazione.

10.1.5. P33 – Politica di monitoraggio, audit e conformità: disciplina la convalida e il riesame di audit delle registrazioni e delle violazioni relative alla gestione delle modifiche.

10.2. Tali politiche, nel loro insieme, consentono un ciclo di vita della gestione delle modifiche nel quadro del SGSI che sia difendibile, tracciabile e sicuro.

11. Standard e quadri di riferimento

11.1. ISO/IEC 27001:2022

11.1.1. Clausola 6.1 – Azioni per affrontare rischi e opportunità: la presente politica supporta l'identificazione, la valutazione e il controllo dei rischi connessi alle modifiche.

11.1.2. Clausola 5.15 – Controllo degli accessi: garantisce che l'accesso durante le modifiche sia controllato e tracciabile.

11.1.3. Appendice A, Controllo 8.32 – Gestione delle modifiche: la presente politica attua pienamente il requisito di gestire le modifiche alle strutture e ai sistemi di elaborazione delle informazioni in modo pianificato e controllato.

11.2. ISO/IEC 27002:2022 – Controllo 8

11.2.1. Rafforza l'attuazione di un processo strutturato di gestione delle modifiche comprendente classificazione, approvazione, test, rollback e documentazione.

11.3. NIST SP 800-53 Rev.5

11.3.1. Famiglia CM (da CM-1 a CM-14): la presente politica è strettamente allineata ai controlli di gestione della configurazione, incluse le configurazioni baseline (CM-2), il controllo delle modifiche di configurazione (CM-3), l'analisi dell'impatto sulla sicurezza (CM-4) e le restrizioni di accesso (CM-5).

11.3.2. Famiglia AU (AU-2, AU-6, AU-12): i meccanismi di logging e audit richiamati nella presente politica supportano la tracciabilità degli eventi e il riesame della conformità per le attività correlate alle modifiche.

11.3.3. RA-3, RA-5: le valutazioni del rischio attivate dalle modifiche e le scansioni di vulnerabilità sono integrate nel processo di valutazione della modifica.

11.3.4. PM-11 (Definizione della missione/dei processi aziendali): garantisce che la continuità operativa e gli obiettivi operativi siano preservati durante le modifiche.

11.4. GDPR UE (2016/679)

11.4.1. Articolo 32(1)(b–d): la presente politica supporta il requisito di misure tecniche e organizzative adeguate per garantire la sicurezza dei dati, in particolare durante le modifiche di sistema.

11.4.2. Articolo 25 – Protezione dei dati fin dalla progettazione e per impostazione predefinita: garantisce che le modifiche che incidono sui dati personali integrino tutela della privacy e sicurezza nella progettazione e nel rilascio.

11.4.3. Considerando 78: richiede che i titolari del trattamento attuino meccanismi, come le politiche di controllo delle modifiche, per garantire la riservatezza, l'integrità e la resilienza continue dei sistemi di trattamento.

11.5. Direttiva UE NIS2 (2022/2555)

11.5.1. Articolo 21(2)(a, b, d, e): impone misure tecniche e organizzative per la gestione dei rischi ICT, inclusi quelli derivanti da modifiche ai sistemi, aggiornamenti software e modifiche infrastrutturali.

11.6. DORA UE (2022/2554)

11.6.1. Articolo 5 – Governance e quadro di controllo interno: la presente politica applica principi di gestione del rischio operativo connessi alle modifiche e agli aggiornamenti ICT.

11.6.2. Articolo 8 – Quadro di gestione del rischio ICT: impone ai soggetti finanziari di gestire tutte le modifiche che incidono sui sistemi ICT tramite processi strutturati di gestione delle modifiche, riflessi nella presente politica attraverso obblighi di classificazione, test, rollback e documentazione.

11.6.3. Articolo 12 – Segnalazione degli incidenti: garantisce che le modifiche non riuscite che causano disservizi ICT siano tracciabili, documentate e segnalate ove applicabile.

11.7. COBIT 2019

11.7.1. BAI06 – Managed IT Changes: la presente politica soddisfa direttamente gli obiettivi BAI06 stabilendo workflow strutturati per approvazione delle modifiche, valutazione dell'impatto, comunicazione e test.

11.7.2. BAI02 – Managed Requirements Definition e BAI03 – Managed Solutions Identification and Build: garantiscono che le modifiche guidate dal business siano riesaminate e attuate in sicurezza.

11.7.3. DSS01 – Managed Operations: supporta l'integrità continua dei sistemi durante l'esecuzione delle modifiche.

11.7.4. MEA01 e MEA03 – Monitor, Evaluate, and Assess Performance and Compliance: consentono una supervisione continua dell’efficacia e dell’applicazione della politica di gestione delle modifiche.